学校编码：10384　　分类号＿＿＿密级＿＿＿

学号：X2010230669　　UDC ＿＿＿

工 程 硕 士 学 位 论 文

税务信息系统安全防护体系研究

Research on Security and Protection System for Tax Information System

张国栋

指导教师姓名： 董槐林 教授

专 业 名 称： 软 件 工 程

论文提交日期：2012 年 10 月

论文答辩时间：2012 年 11 月

学位授予日期： 年 月

答辩委员会主席：＿＿＿＿＿

评 阅 人：＿＿＿＿＿

2012 年 10 月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下,独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

年　　月　　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（　√　）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年　　月　　日

摘要

信息安全是国家安全的重要组成部分。随着税务系统数据实现大集中，网站、网上办税等基于互联网的税收信息化快速发展，税务信息系统覆盖了税收征管的方方面面。多元化征收方式使跨部门的横向沟通不断增加，税务系统的信息安全风险不断增加，信息安全已引起各级税务部门的高度重视。信息安全不仅关系到税务机关税收征管业务的正常开展，还直接影响到税务系统的纳税服务水平和税务部门形象。

税务网络系统是税务信息系统运行的物理基础，保护税务网络系统安全运行是税务信息系统发挥正常效能的关键。税务网络系统结构包括广域网和内部局域网，税收活动通过税务系统的终端进入系统。另外，税收业务还可以直接面向社会，通过与公共网络进入体系，实现税务服务。从这个网络结构来看，建设专门的监管使用的监控网络系统和监控网络的运营管理系统是必要的。所以说，税收监管现代化和信息化建设任务依然艰巨，是信息化建设的重要新领域，为信息安全产业开辟了新的市场前景。

论文以动态安全防护模型为理论依据，以所采用的各种安全技术为支撑，以税务安全防护系统为蓝本，通过深入分析各类网络安全隐患及信息所面临的安全风险，探讨适合于税务信息系统安全防护体系为最终目的与解决方案。

关键词：信息安全；信息监管；防护体系

Abstract

Information security is an important part of national security. Along with the centralization of tax system data are realizing, the website and tax online based on the Internet are developed rapidly, the tax information system covers all aspects of the tax collection and management, plurality of collect taxes methods make cross-sectional lateral communication be increased，information security risk of the tax system is increasing constantly, information security has aroused great attention of the tax authorities at all levels. Information security is not only related to the normal the taxation administration business, but also affect the tax system tax service level and the tax department image directly.

The tax network system is the physical basis of tax information system, Protection of network system safety is the key of tax information system display its potency. Network structure of tax system includes the production of stem network and internal node network, tax activities access system through the tax system terminal. In addition, tax business can also facing the society with the public network into the system in order to realize tax services.

The construction supervision of the special use monitoring network system and monitoring network operation management system is necessary from this network structure view. Therefore, tax regulatory modernization and information construction is still an arduous task and the information construction important new field for the information security industry has opened up new market prospects.

The research is based on security protection model with the various technical support used by network and information security protection system, we'll discuss a set of suitable tax information security guarantee system based on tax security protection system through in-depth analysis of various kinds of network security and information security risk as the final goal and the solutions.

Key Words: Information Security; Information Monitoring and Management; Protection System

目 录

第一章 引言 1

1.1 背景概述 1

1.2 选题意义 1

1.3 国内外信息安全技术发展现状 2

1.4 研究内容介绍 3

第二章 信息安全相关理论与技术 5

2.1 信息与信息安全 5

2.1.1 信息 5

2.1.2 信息安全 5

2.1.3 信息安全体系结构 6

2.1.4 安全防护模型 7

2.2 信息安全防护相关技术 10

2.2.1 防火墙 10

2.2.2 网闸（物理隔离器）技术 11

2.2.3 网络加密技术 15

2.2.4 入侵检测和防御 17

2.2.5 桌面管理系统 19

2.2.6 准入系统 21

2.2.7 安全审计系统 21

2.2.8 虚拟局域网 22

2.2.9 加密和身份认证技术 24

2.3 本章小结 26

第三章 税务信息系统安全需求分析 27

3.1 信息安全策略 27

3.1.1 保护对象 27

3.1.2 安全策略 27

3.2 信息安全建设现状 28

3.2.1 物理安全建设 28

3.2.2 网络安全建设 28
3.2.3 系统安全建设 29
3.2.4 应用安全建设 29
3.2.5 组织机构与安全制度 29
3.3 税务信息系统面临的威胁 30
3.3.1 威胁的来源 30
3.3.2 威胁的方法 31
3.4 税务信息系统安全风险分析 32
3.4.1 物理层面的安全风险 32
3.4.2 网络层面的安全风险 33
3.4.3 系统层面的安全风险 35
3.4.4 应用层面的安全风险 36
3.4.5 管理层面的安全风险 39
3.5 本章小结 40
第四章 安全防护体系总体设计 41
4.1 理论基础 41
4.2 信息安全防护体系 42
4.2.1 总体目标 42
4.2.2 基本内容 43
4.2.3 安全机制 44
4.3 体系框架 45
4.3.1 总体架构 45
4.3.2 层次及相互关系 48
4.3.3 拓扑结构 49
4.4 税务安全防护系统 51
4.4.1 第一期安全防护系统 51
4.4.2 第二期安全防护系统 52
4.4.3 第三期安全防护系统 52
4.5 本章小结 53

第五章 安全防护体系详细设计 54

5.1 税务局域网内的安全域划分.....54

5.2 网络安全架构.....55

5.2.1 网络设备的安全配置 55

5.2.2 网络边界防护配置 56

5.3 防护系统配置.....57

5.3.1 防火墙 57

5.3.2 网闸部署 63

5.3.3 入侵检测 64

5.3.4 桌面防护系统 67

5.3.6 安全审计系统 70

5.4 安全防护系统管理平台设计.....72

5.4.1 设计目标 72

5.4.2 设计原则 73

5.4.3 设计要求 73

5.4.4 系统组成和主要功能 74

5.4.5 安全管理流程 79

5.5 本章小结.....81

第六章 总结与展望 82

6.1 总结.....82

6.2 展望.....82

参考文献.....80

致谢.....85

Contents

Chapter 1 Introduction 1

1.1 Background 1

1.2 Significance 1

1.3 Development Status of Information Security Technology in China and Abroad 2

1.4 Research Contents 3

Chapter 2 Theory and Technology of Information Security 5

2.1 Information and Information Security 5

2.1.1 Information 5

2.1.2 Information Security 5

2.1.3 Information Security Architecture 6

2.1.4 Security protection model 7

2.2 Information Security Technology 10

2.2.1 Firewall 10

2.2.2 GAP (Physical Isolator) Technology 11

2.2.3 Network Encryption Technology 15

2.2.4 Intrusion Detection and Prevention 17

2.2.5 Desktop Management System 19

2.2.6 Access System 21

2.2.7 Security Audit System 21

2.2.8 Vlan 22

2.2.9 Encryption and Identity Authentication Technology 24

2.3 Summary 26

Chapter 3 Requirements Analysis of Information Security 27

3.1 Information Security Policy 27

3.1.1 Protection Object 27

3.1.2 Security Policy 27

3.2 Status of Information Security 28

3.2.1 Physical Security Construction 28

3.2.2 Network Security Construct 28

3.2.3 System Security Construct 29

3.2.4 Application Security Construct 29

3.2.5 Organization and Security Institution....29
3.3 The Threat on Tax Information System....30
3.3.1 The Source of Threat....30
3.3.2 The Method of Threat....31
3.4 Risk Analysis about Tax Information System....32
3.4.1 Physical Security Risk....32
3.4.2 Network Security Risk....33
3.4.3 System Security Risk....35
3.4.4 Application Security Risk....36
3.4.5 Organization and Security Risk....39
3.5 Summary....40
Chapter 4 The Overall Design of Security and Protection System....41
4.1 Theory Foundation....41
4.2 Information Protective System Architecture....42
4.2.1 Overall Goal....42
4.2.2 Basic Contents....43
4.2.3 Security Mechanism....44
4.3 System Architecture....45
4.3.1 Architecture....45
4.3.2 Levels and Relationship....48
4.3.3 Topology Structure....49
4.4 Security Protection System of Tax....51
4.4.1 The First Period of Security Protection System....51
4.4.2 The Second Period of Security Protection System....52
4.4.3 The Third Period of Security Protection System....52
4.5 Summary....53
Chapter 5 The detailed design of Security and Protection System....54
5.1 LAN Security Domain of Tax System....54
5.2 Network Security Architecture....55
5.2.1 Security Configuration of Network Equipment....55
5.2.2 Security Configuration of Network Boundary....56
5.3 Protective System Configuration....57
5.3.1 Firewall....57

5.3.2 GAP 63
5.3.3 Intrusion Detection System 64
5.3.4 Desktop Management System 67
5.3.6 Security Audit System 70
5.4 Security System Design of Management Platform 72
5.4.1 Design Objective 72
5.4.2 Design Principles 73
5.4.3 Design and Requirements 73
5.4.4 Composition and Main Function of System 74
5.4.5 Security Management Process 79
5.5 Summary 81
Chapter 6 Conclusions and Propect 82
6.1 Conclusions 82
6.2 Propect 82
References 84
Acknowledgements 85

第一章 引言

1.1 背景概述

随着我国经济的持续发展和国际地位的不断提高，我国的基础信息网络和重要信息系统面临的安全风险日益严峻，计算机病毒传播和网络非法入侵十分猖獗，网络违法犯罪持续大幅上升，犯罪分子利用一些安全漏洞，使用黑客病毒技术、网络钓鱼技术、木马间谍程序等新技术进行网络盗窃、网络诈骗、信息系统破坏等违法活动，给我国政治、经济和社会生活造成严重负面影响。

近十年来，我国税务信息化建设取得了突飞猛进的发展，税收工作已由前期以替代手工操作为主的简单计算机应用逐步向全面监控税收管理各个环节转变，应用的深度得到前所未有的拓展，税收工作对计算机网络系统的依赖已经达到了空前的程度。税务系统信息化建设由于发展速度较快，所面临的信息安全方面的风险也越来越大。由于信息安全系统的建设明显滞后于信息系统本身的规划和建设，整个税务信息系统没有形成一个完整的信息安全防护体系，对于税收工作至关重要的税务计算机信息的安全正在受到来自各方面的威胁和挑战。税务信息系统作为我国重要信息系统之一，其安全运行不仅关系到各级税务机关税务工作的正常开展和全国税务机关的形象，还将影响到国家的安全和社会的稳定。

1.2 选题意义

税收信息化建设的不断发展，使税收的各项工作都离不开计算机网络，如税务部门征收、管理、稽查，纳税人多元化网络报税、发票认证等。计算机网络给税收工作带来的便利是不言而喻的，但税务网络和重要信息系统所面临的安全风险日益严峻。为防范来自税务信息系统之外的安全风险，保护信息系统的安全，提高税务信息系统的可用性，需要采取必要的安全防护措施。通过配置防火墙加强了网络边界保护，通过配置入侵检测系统加强了网络流量的安全监测，通过配置网络防病毒系统加强了网络运行环境的基本保护。对外防护的同时，应更加注重对内的管理。统计数据表明，80%的安全问题来自于内部网络，而内部网络的主要安全问题是计算机终端的违规接入、违规操作以及病毒问题，因此必须要加倍重视内部网络的安全防护，加强内部网络安全防护建设力度。为最大程度的保障税务信息安全，充分考虑税务信息系统的安全需求，以加强内部网络安全防护为重点，通过部署安全审计系统、局域网桌面安全防护产品和病毒集中预警管理

系统等技术产品，改善税务系统专网计算机系统的安全性、可审计性和可控性。自外而内筑造强大的安全防线。

1.3 国内外信息安全技术发展现状

从国际、国内信息安全技术发展情况来看，安全技术朝着构成一个完整、联动、快速响应的防护系统方向发展，采用系统化的思想和方法构建信息系统安全防护体系成为一种趋势。安全技术逐步由传统的被动防御向主动式预防和防护发展，可信计算、主动式恶意代码防护等技术日益受到重视。网络和信息系统性能的不断提高，需要网络安全产品不断提高性能以满足高速、高性能环境下的安全保护需求。随着网络和信息系统日趋复杂，必须将信息安全技术依据一定的安全体系设计进行整合、集成，达到综合防范的要求。信息安全技术也日益融合到信息技术产品和系统中[1]。

目前全球信息安全产业发展水平较高的国家主要有美国、法国、以色列、英国、日本等，与国际先进水平相比，我国信息安全行业的技术水平具有如下特点：

1、关键核心技术与国际先进水平差距不大。

信息安全领域的核心技术可以分成结构性技术和解构性技术两大类，我国在这两类技术层面与国际先进水平差距不大。

（1）结构性技术，即体系化技术，典型代表为加密认证技术，其核心内涵就是为防御体系和保障体系构建各个要素之间的紧密关联。以加密认证技术等为基础形成的网络安全域理论和方法，就是在网络和系统层面的将网络设备节点、链路、服务器、客户端等等组成一个结构性体系，以抵抗攻击、保障服务能力、增加强壮性。我国在加密认证技术研究和应用的许多细分领域已经达到国际先进水平：如在数据加密和加密设备研究方面，江南计算机研究所和科学院等单位参与和自主开发的十几万亿次的计算机和具有数百 T 以上规模的存储设备已经达到世界先进水平；在身份认证、数字证书及其管理技术方面取得了许多应用成果；在密码技术方面，国内专家破译 MD5 算法成为我国密码技术水平的突出代表。

（2）解构性技术，其中最主要的就是攻防对抗技术。对信息安全系统构成威胁的攻击技术是一种突破防御体系、将保障体系进行解构的力量，而防御攻击的技术核心是检测技术，如防病毒系统的首要功能是对病毒文件的检测；防火墙则是一个对数据包进行甄别和判断的检测设备；入侵检测系统更是对于网络和系统攻击数据包的检测。为了提高检测技术和检测设备的水平，则首先要对攻击技

术有非常深入的了解。在攻防对抗技术领域，我国信息安全产业的技术水平与国际保持同步，在漏洞检测、网络攻击方法、攻击防御等方面与世界水平相当甚至有所超越，并形成了某些专有技术。在产品研发方面，相当一批民营企业已能够成团队地开展攻防技术的体系化研究和产品化开发；在以攻击技术和检测技术为内涵的安全服务领域中，我国信息安全产业完全可以和国际先进水平进行抗衡。

2、安全技术转化为产品的能力与国际先进水平有差距。

在信息安全主流产品（防病毒、防火墙、IDS/IPS、漏洞扫描、加密、UTM、SOC 等）方面，我国尚无真正能打入国际主流市场的国际化安全产品，在产品成熟度、国际市场占有率、国际品牌影响力等方面与国际先进水平有差距。但是在国内信息安全产品市场，国内企业能够在不同的细分市场中占据领先地位或与国外产品抗衡。造成产品层面差距的原因除技术差距外，还主要在于整个产业的产品化能力和国际营销能力不足，产业链相关上下游行业的综合实力有待提高。

3、安全技术迅速融入服务的能力与国际先进水平相当。

由于信息安全所具有的对抗特性、对信息系统的密切关联性、安全技术和产品应用的复杂性等等，使得安全服务在整个信息安全领域中占据了非常重要的地位。信息安全服务通常包括：系统和网络风险评估和加固、信息安全管理体系咨询和认证、渗透性测试、系统集成、运维、应急、培训等。安全服务主要依靠人和人的活动来完成，因此信息安全的核心技术可以比较直接地应用于安全服务。决定安全服务水平高低的是服务整体的产能管理、项目群管理等方面的能力。我国企业和国际一流企业在安全服务水平，以及从客户能够实际获得的服务价值方面差距并不大，在有些服务门类上，我国企业还能够根据国情为本国企业提供更贴切的优质服务[2]。

1.4 研究内容介绍

税务信息系统由服务器、个人计算机、打印机等其他终端设备和连接它们的网络系统构成。国家税务机关的网络系统一般分为内网和外网。各级税务机关内网是全国税务系统重要的组成部分之一，承载着税收业务、行政办公等类业务应用系统。内网连接着全国所有的省级国税局和地税局，这种连接称为纵向连接；内网还连接着人民银行、海关、公安、质检、市委市府等其它机构，这种连接称为横向连接。外网连接着互联网，承载着网上办税系统和 12366 税收服务系统，向广大纳税人和社会提供纳税申报、税款征收和税收政策咨询等服务，还承载着

电子邮件等互联网应用系统。

本文的探索以税务信息系统为研究对象，以所承载的税务信息为保护重点，以动态安全防护模型为理论基础。研究方法上，通过深入分析税务信息系统所面临的安全风险和隐患，将信息系统安全风险划分为外部风险和内部风险两部分，分别进行布控。降低外部风险以安全防护技术为主，降低内部风险以安全管理技术为主。通过对防火墙、入侵监测、防病毒和漏洞扫描、桌面系统、准入系统、安全审计等目前比较流行的安全产品的理论阐述，研究各系统协调运行和整体联动，为构建有一定强度的、可动态调整的信息安全防护系统，真正意义上实现内部和外部风险的双重防护做一些努力，探讨适合于税务信息系统安全防护体系为最终目的与解决方案。

第二章主要包括与论文相关的概念叙述和安全产品技术介绍，详细论述了基础动态模型的原理，并引入增强型动态模型作为继续研究的理论依据，并对该模型做了说明；

第三章立足税务信息系统的建设现状，阐述了税务信息系统面临的威胁，分析了税务信息系统安全所面临的风险，为后期研究做好铺垫；

第四章以动态增强型信息安全模型为构建税务信息系统安全防护体系的理论基础，阐述了税务信息系统安全防护体系的构建要素和系统组成，并对其重要组成部分税务安全防护系统的建设情况做了叙述；

第五章为论文的实现部分，针对税务信息系统安全防护，主要叙述安全产品的具体部署，并对安全防护系统管理平台做了初步设计；

第六章对本文的研究工作做了总结，明确了进一步研究工作的方向。

第二章 信息安全相关理论与技术

信息安全的实质就是要保护网络系统所承载的信息资源免受各种类型的威胁、干扰和破坏，即保证信息的安全性。根据国际标准化组织的定义，信息安全性的含义主要是指信息的完整性、可用性、保密性和可靠性。信息安全是任何国家、政府、部门、行业都必须十分重视的问题，是一个不容忽视的国家安全战略。对于税务部门而言，需要重点保护的信息包括：涉及国家秘密的信息、内部工作文件（包括起草中未发布的政策性文件）、业务数据（如纳税人的涉税信息、发票信息、统计分析数据等）、内部行政信息（如人事、财务、纪检、监察等信息）、其它不宜公开或遭到破坏后严重影响工作的内部信息。信息安全的基础知识、信息安全模型、当代主流的安全防护技术，如防火墙、物理隔离网闸、入侵检测和防御、桌面安全管理、终端准入、网络安全审计、VLAN、加密和身份认证等技术是研究安全防护体系必须掌握的技术。本章内容主要是理清概念和掌握防护方法，为后续进一步研究奠定理论和技术基础。

2.1 信息与信息安全

2.1.1 信息

信息是通过施加于数据上的某些约定而赋予这些数据的特定含义。信息本身是无形的，借助于信息媒体以多种形式存在或传播，可以存储在计算机、磁带、纸张等介质中，也可以记忆在人的大脑里，还可以通过网络、打印机传真机等方式进行传播。通常情况下可以把信息理解为信息、信号、数据、情报、知识等[3]。

2.1.2 信息安全

信息安全的概念与信息的安全属性密不可分，保密性、完整性、可用性（通常称为 CIA）是信息的三大安全属性，除此之外，还有可控性、不可否认性等其它属性。

1、保密性

信息的保密性是指保证只有被授予特定权限的人才能访问到信息。信息的保密性依据信息被允许访问对象的多少而不同，所有人员都可以访问的信息为公开信息，需要限制访问的信息为敏感信息或秘密信息。根据信息的重要程度和保密要求可以将信息分为不同保密等级。已授权用户根据所授予的权限可以对信息进行操作，有的用户只可以读取信息，有的用户则可以进行读写操作。